

Руководство пользователя системы Infozorok

Содержание

Перечень условных обозначений и сокращений.....	3
1.Возможности системы	4
2.Начало работы	5
Общие принципы.....	5
Интерфейс, модули и коллекции	5
Инструменты	6
Поиск.....	6
Объединяющая коллекция	7
Связи между коллекциями	8
Настройка столбцов	8
Закладки.....	10
Импорт/экспорт данных	10
Профиль пользователя.....	10
3.Модули системы.....	11
3.1.Модуль Кадры.....	11
Коллекция Person	12
Коллекция Employee.....	13
Коллекция Structure	14
Коллекция Absence	15
Коллекция Anketa.....	16
Коллекция Spravka.....	17
3.2.Модуль Активы.....	18
Коллекция Asset	19
3.3.Модуль Учетные записи	20
Коллекция Account.....	21
3.4.Модуль Склад	22
Коллекция Stock.....	23
3.3.Модуль Документы	24
Коллекция Документы.....	24
3.4.Модуль Инциденты	25
Коллекция Инциденты	25
3.5.Модуль Задачи	26
Коллекция Задачи	26
4.Контактная информация.....	27

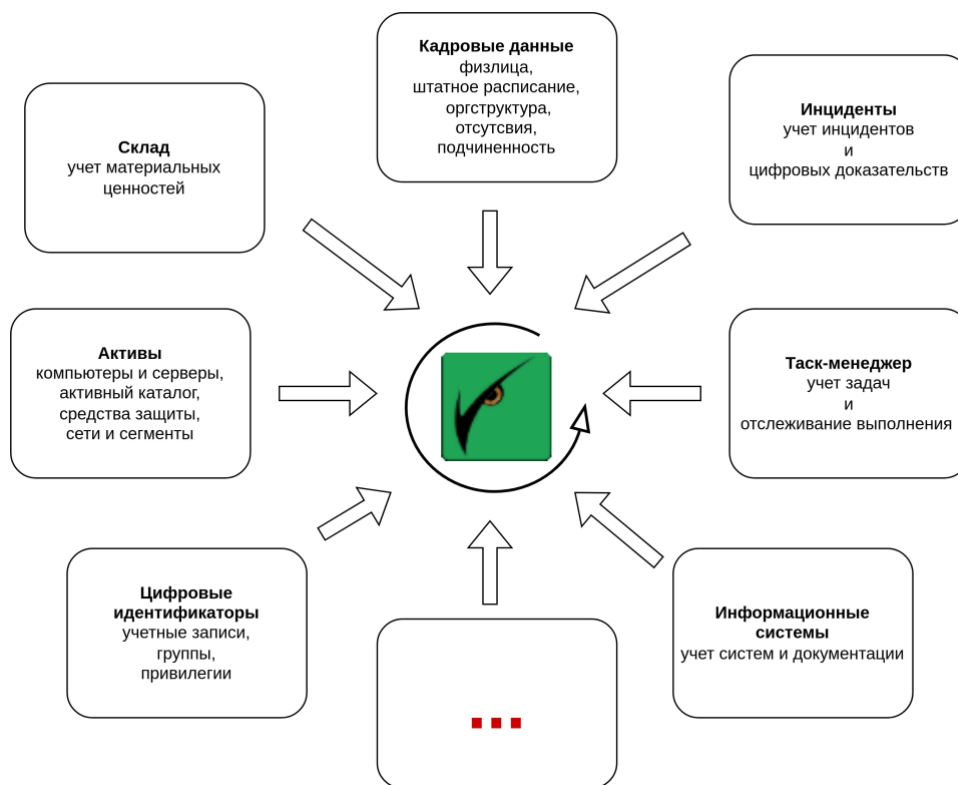
Перечень условных обозначений и сокращений

Модуль	Логическое объединение данных в системе в соответствии с выполняемым функционалом
Коллекция	Единица организации данных в системе, аналог таблицы в базе данных
Объект коллекции	Запись в коллекции системы, аналог строки в таблице базы данных
Объединяющая коллекция	Особый тип коллекции, которая связывает коллекции-источники по общему признаку и отображает информацию в едином интерфейсе, аналог сводной таблицы

1. Возможности системы

Система информационной безопасности InfoZorok - это программное решение, которое интегрирует несколько функций безопасности в единую платформу.

Выполняет такие задачи как инвентаризация и управление ИТ-активами, контроль конфигураций, управление событиями, а так же централизованный сбор и анализ данных за счет интеграции с другими системами информационной безопасности.

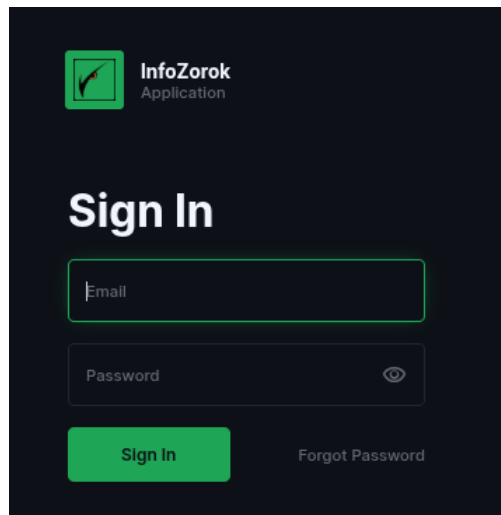


Гибкая структура решения позволяет оперативно добавлять новый функционал. Имеет единую консоль, что обеспечивает централизованной контроль различных аспектов безопасности.

Система предоставляет возможность улучшить защиту за счет комплексного подхода к безопасности. Это помогает снизить сложность управления безопасностью и повысить эффективность обнаружения и реагирования на угрозы.

2.Начало работы

Для доступа к интерфейсу системы необходимо перейти по адресу, где опубликован web-сервер системы (<https://<адрес сервера>/admin/login>). Далее ввести логин, пароль и второй фактор, если он установлен обязательным для вашей учетной записи.



Общие принципы

Работа системы состоит из трех основных этапов:

- 1.Импорт, подготовка, связывание и хранение, визуализация данных
- 2.Мониторинг
- 3.Автоматизация

Для выполнения первого этапа настраиваются интеграции с внешними системами – источниками данных. В результате система, с помощью одного или нескольких своих агентов, автоматически обогащается данными, предварительно обрабатывает их и сохраняет в своей базе. После чего для пользователя доступна визуализация и при необходимости возможность вручную дополнять полученные данные.

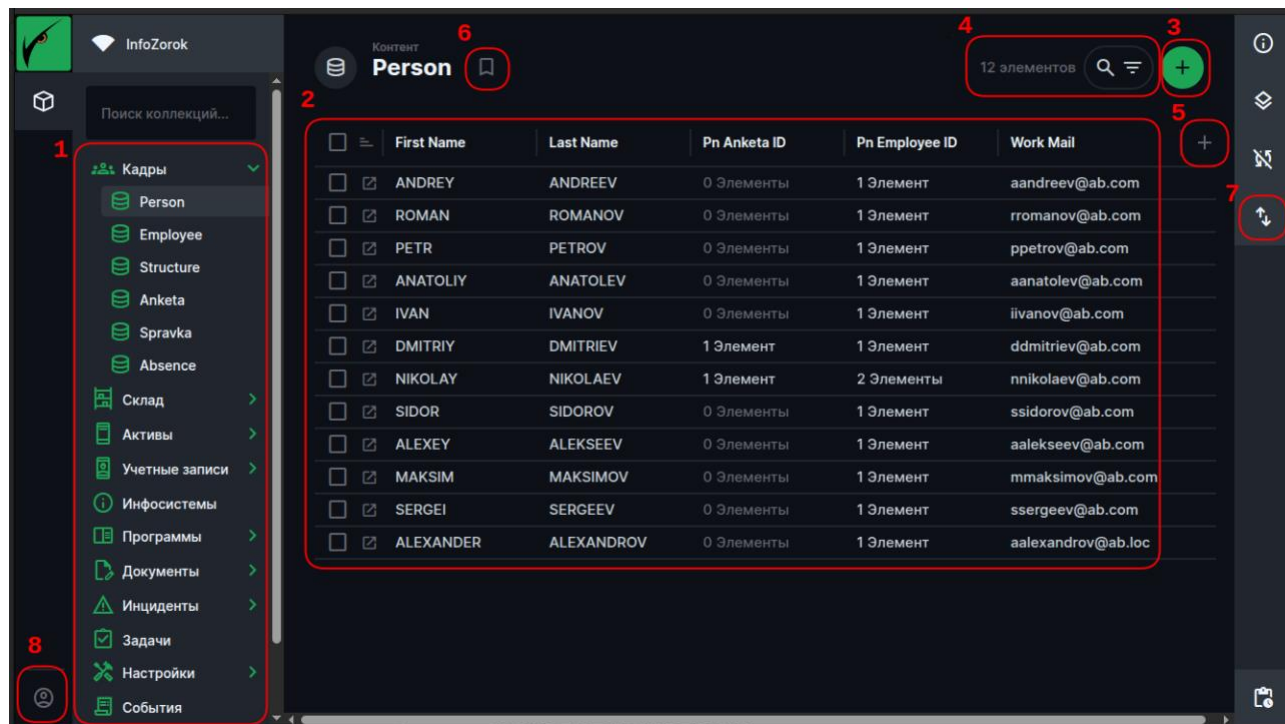
На этапе мониторинга настраиваются сигнатуры для автоматизированного поиска несоответствий и отклонений от заданного состояния. Сгенерированные алерты могут направляться пользователю на электронную почту или в Telegram, в соответствии с заданными настройками администратором системы.

На третьем этапе система позволяет настраивать автоматизированные ответные действия в систему-источник.

Интерфейс, модули и коллекции

Интерфейс пользователя состоит из следующих основных инструментов:

- 1.панель модулей и коллекций
- 2.поле для отображения содержимого коллекции
- 3.добавление нового объекта коллекции
- 4.меню поиска
- 5.меню настройки отображения столбцов
- 6.создание закладок
- 7.импорт/экспорт данных
- 8.профиль пользователя



Основные сущности в системе это:

- Модули
- Коллекции
- Объекты коллекций

Каждый Модуль в системе выполняет свой определенный функционал. Модуль может содержать одну и более Коллекций, которые хранят в себе данные. Данные коллекции представлены в виде Объектов этой коллекции.

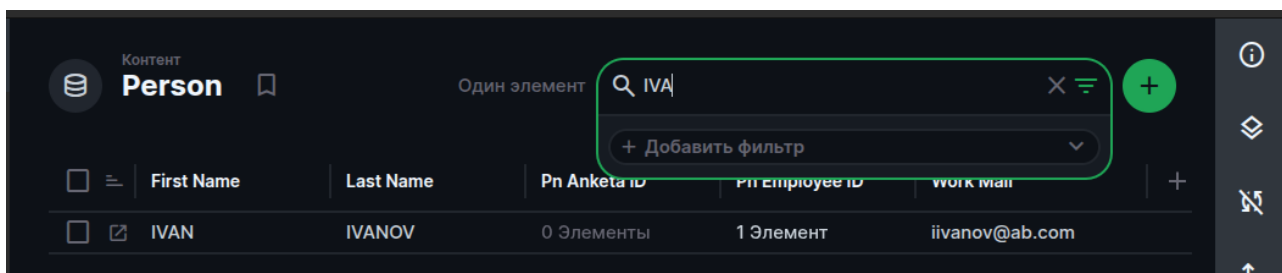
Например, модуль Кадры, который содержит коллекции Person (физические лица), Employee (работники), Structure (штатная структура) и т. д. Коллекция Person, в свою очередь, содержит объекты — записи о физлицах, например ANDREY ANDREEV.

Инструменты

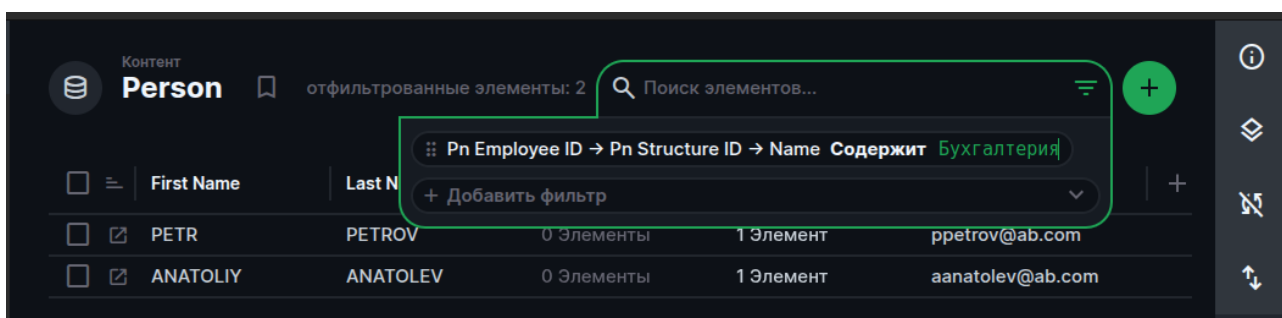
Поиск

Позволяет искать объекты как по столбцам выбранной коллекции, так и по дочерним коллекциям.

Например, для поиска физлица по ФИО в коллекции Person, достаточно ввести фамилию в поле поиска:

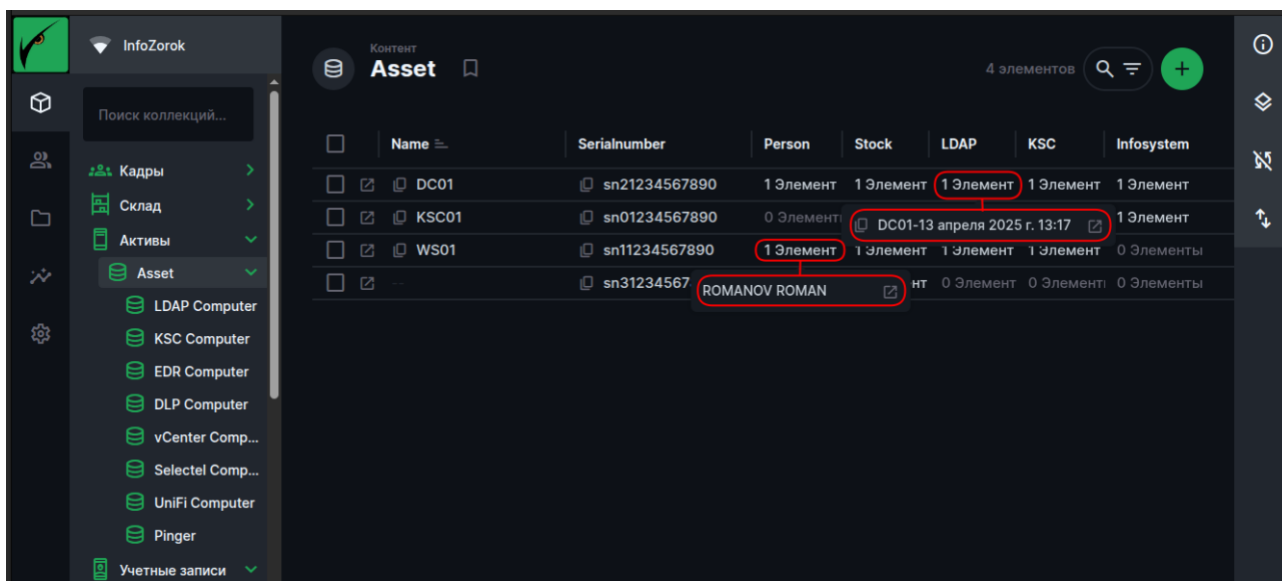


Если же необходимо выполнить поиск по столбцу связанной коллекции, то нужно нажать Добавить фильтр в меню поиска и ввести интересующую коллекцию и столбец, по которому будем искать. Например, необходимо из коллекции Person найти физлиц, работающих в Бухгалтерии. На рисунке ниже изображен фильтр, который позволяет это сделать.



Объединяющая коллекция

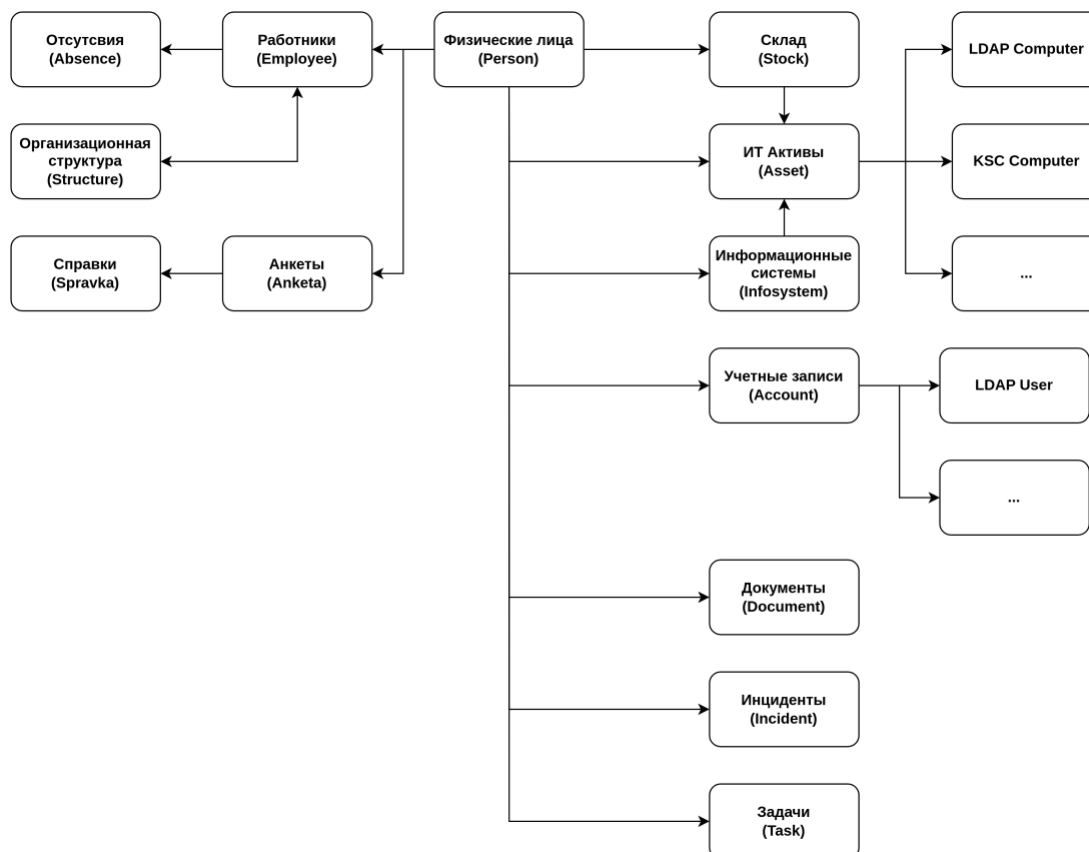
Связывает коллекции по общему признаку и отображает информацию в едином интерфейсе. На рисунке ниже показана объединяющая коллекция Активы (Asset), которая объединяет дочерние коллекции-источники данных о компьютерах из таких систем как каталог LDAP, антивирус Касперского и др. Это позволяет оперативно получать информацию из коллекции-источника, переходя по соответствующим ссылкам.



Связи между коллекциями

Связи позволяют логически объединять между собой коллекции, содержащие информацию из первоисточников, и получать целостную картину всех объектов в системе.

На рисунке изображены коллекции и связи между ними:



Каждая коллекция может иметь одну и более связей. Например, в компании работает IVAN IVANOV, информация о котором содержится в объекте коллекции Физические лица (Person). Он трудоустроен в должности системного администратора, информация об этом содержится в объекте коллекции Работники (Employee). Эти объекты связаны друг с другом. Далее можно назначить физлицо IVAN IVANOV материально ответственным за физический сервер, находящийся на складе, которому соответствует объект в коллекции Склад (Stock). Сервер имеет учетную запись в активном каталоге LDAP (объект коллекции LDAP Computer) и запись в антивирусной системе Kaspersky (объект коллекции KSC Computer), которые в свою очередь связаны Объединяющей коллекцией ИТ Активы (Asset), где содержится соответствующий объект.

Настройка столбцов

Позволяет выбрать оптимальный набор данных (столбцов) для отображения в интерфейсе коллекции. На рисунке ниже показано как добавить отображение рабочей электронной почты физлица. Есть возможность добавления в столбцы из дочерних коллекций.

Контент **Person** 12 элементов

	First Name	Last Name	Pn Anketa ID	Pn Employee ID	
☐	ANDREY	ANDREEV	0 Элементы	1 Эле	Work Mail
☐	ROMAN	ROMANOV	0 Элементы	1 Эле	Telephone Number
☐	PETR	PETROV	0 Элементы	1 Эле	When Created
☐	ANATOLIY	ANATOLEV	0 Элементы	1 Эле	Address
☐	IVAN	IVANOV	0 Элементы	1 Эле	Account
☐	DMITRIY	DMITRIEV	1 Элемент	1 Эле	Asset
☐	NIKOLAY	NIKOLAEV	1 Элемент	2 Элемента	

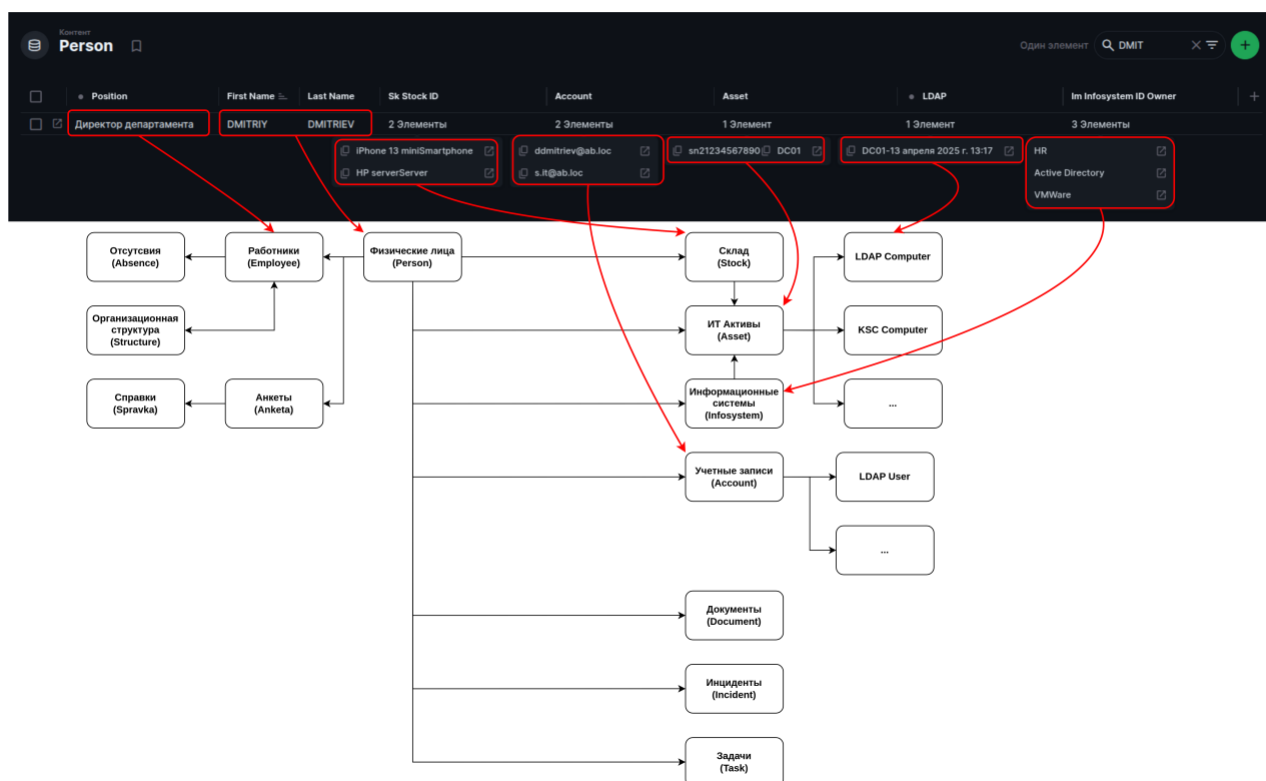
Контент **Person** 12 элементов

	First Name	Last Name	Pn Anketa ID	Pn Employee ID	Work Mail
☐	ANDREY	ANDREEV	0 Элементы	1 Элемент	aandreev@ab.com
☐	ROMAN	ROMANOV	0 Элементы	1 Элемент	rromanov@ab.com
☐	PETR	PETROV	0 Элементы	1 Элемент	ppetrov@ab.com
☐	ANATOLIY	ANATOLEV	0 Элементы	1 Элемент	aanatolev@ab.com

Далее, с помощью настройки столбцов и зная как связаны между собой коллекции, можно вывести необходимую консолидированную информацию в едином интерфейсе.

Ниже приведен пример вывода консолидированных данных о:

- работнике, его должности
- материальных ценностях
- учетные записи работниками
- связанные ИТ активы
- учетные записи компьютеров и серверов, относящихся к активам
- информационные системы, владельцем которых является пользователь



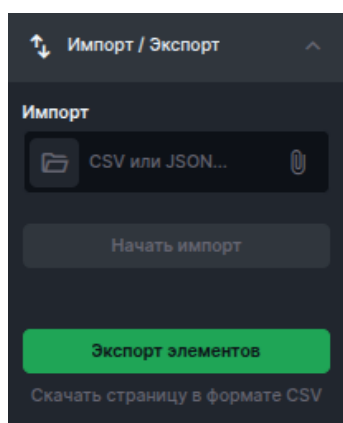
Закладки

После настройки отображения интерфейса и необходимых фильтров, в системе предусмотрена возможность сохранить изменения путем создания закладки.

Импорт/экспорт данных

Для использования информации коллекций вне системы, предусмотрена возможность экспорта (импорта) данных в CSV или JSON.

Ниже показан интерфейс, где необходимо выбрать целевой файл, нужные столбцы коллекции, после чего можно выполнить импорт/экспорт данных.



Профиль пользователя

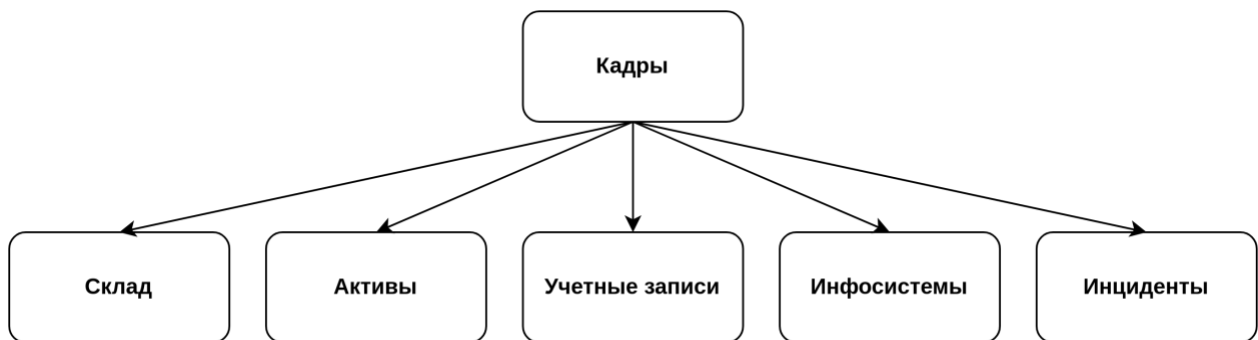
В профиле предусмотрена возможность посмотреть персональные настройки пользователя и изменить параметры отображения, например язык интерфейса и тему.

3. Модули системы

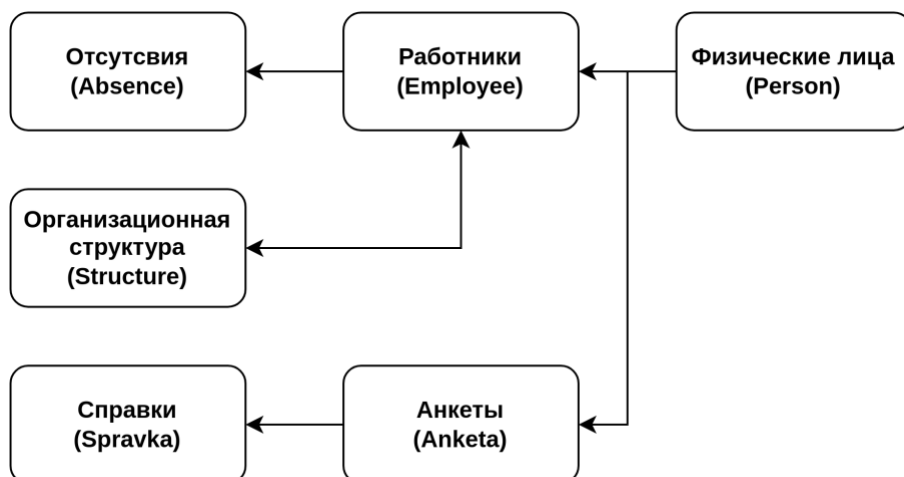
Как было указано ранее система состоит из нескольких преднастроенных модулей — логических единиц, функционально объединяющих коллекции в системе. Далее будут описаны модули и коллекции внутри каждого из них.

3.1. Модуль Кадры

Модуль Кадры является одним из основных модулей системы, функцией которого является назначение и контроль ответственных за объекты в системе. Кадровый модуль содержит данные из HR-систем компании и имеет связи с остальными модулями.



Все коллекции внутри модуля Кадры взаимосвязаны. Условно, связи можно представить так:

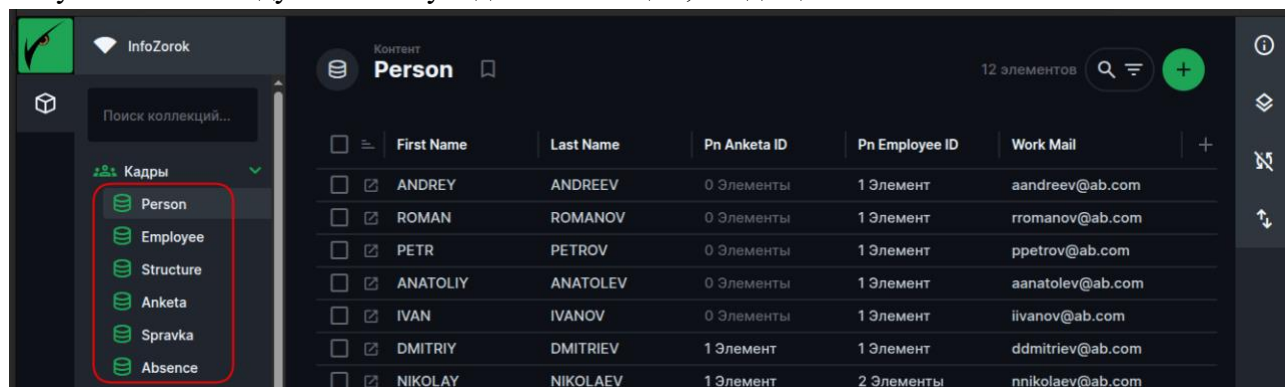


Благодаря структуре связей система позволяет отслеживать такие события как:

- приемы
- переводы в другие подразделения
- увольнения

- подчиненность как на уровне руководитель-подчиненный, так и на уровне штатной структуры.

В пункте меню модуля можно увидеть коллекции, входящие в его состав.



Коллекции модуля Кадры:

- физические лица (Person)
- работники (Employee)
- организационная структура (Structure)
- отсутствия работников, отпуска, прогулы и т.д. (Absence)
- анкеты кандидатов на работу (Anketa)
- справки по проверке анкет кандидатов (Spravka)

Каждая коллекция содержит карточку объекта, с детальной информацией.

Коллекция Person

В карточке физического лица отображается такая информация как:

- ссылка на занимаемую штатную единицу
- ссылка на анкету
- персональные данные
- секция со ссылками, указывающими на ответственность за Учетные записи, Активы, Информационные системы, Оборудование на складе
- секция Инцидентов, с указанием были ли зарегистрированы на данного человека инциденты.

←

Person

Редактирование элемента в Person

Pn Employee ID

ddmitriev@ab.loc ✓

✎

🗑

Создать

Добавить существующий

Pn Anketa ID

DDMITRIEV DMITRIY 1990-01-01

🗑

Создать

Добавить существующий

Last Name

DDMITRIEV

First Name

DDMITRIY

Middle Name

DDMITRIEVICH

Birth Date

1 января 1990 г. ✕

Idnumber

30504830530

Mail

Work Mail

ddmitriev@ab.com

Telephone Number

+79119876543

When Created

🗑

Address

РФ, СПб

Responsibility

Account

ddmitriev@ab.loc

✎

🗑

Добавить существующий

Asset

Нет элементов

Добавить существующий

Im Infosystem ID Owner

HR

✎

🗑

Active Directory

✎

🗑

VMWare

✎

🗑

Добавить существующий

Im Infosystem Admin

Нет элементов

Добавить существующий

Sk Stock ID

iPhone 13 miniSmartphone

🗑

HP serverServer

🗑

Создать

Добавить существующий

Incidents

It Incident ID Intruder

Нет элементов

Создать

Добавить существующий

It Incident ID Head

✎

🗑

Создать

Добавить существующий

Коллекция Employee

В карточке работника отображается следующая информация:

- ссылка на карточку физлица
- организация
- должность
- штатная структура нижележащих подразделений
- активна ли и существует штатная единица
- табельный номер
- дата трудоустройства и увольнения
- руководителем какого подразделения является работник
- кто является руководителем работника и кто находится у него в подчинении
- список документов, с которыми ознакомлен работник
- информация об отсутствиях.

Employee
←
Редактирование элемента в Employee

Pn Person ID
VADIMOV VADIM 4 августа 1980 г.
✎ ✕

Organization
ABRETAIL
▼

Position
Генеральный директор

Pn Structure ID
ABRETAIL ABRETAIL
✎ ✕

Active
☒ Включено

Exist
☒ Включено

Employee ID
222222

Category

Start Date
19 апреля 2020 г.
✕

End Date
📅

When Created
21 апреля 2025 г. 18:09
✕

Pn Structure ID Head
ABRETAIL ABRETAIL
🗑️

Создать

Добавить существующий

ID Head
OLEGOV OLEG AB ✓
✎ ✕

ID Subordinate
VLADISLAVOVA VLADA ABRETAIL ✓
📄 🗑️

Добавить существующий

Automatic
☒ Включено

Document

Dt Document ID
🕒 Нет элементов

Добавить существующий

Pn Absence ID
🕒 Нет элементов

Создать

Добавить существующий

Коллекция Structure

В карточке подразделения отображается следующая информация:

- название родительского подразделения
- название подразделения
- организация
- ссылка на карточку работника – руководителя подразделения
- древовидная структура подразделений, входящих в состав выбранного
- список ссылок на карточки работников, которые числятся в выбранном подразделении

Structure

← Редактирование элемента в Structure

ID Parent

AB AB

Name

ABRETAIL

Organization

ABRETAIL

Pn Employee ID Head

VLADIMIROV VLADIMIR Генеральный директор ✓  

Treeview ID

▼ Департамент безопасности  

▼ Управление информационной безопасности  

▼ Бухгалтерия  

Добавить существующий

Pn Employee ID

VLADIMIROV VLADIMIR Генеральный директор ✓  

Добавить существующий

Коллекция Absence

В карточке отсутствия указывается:

- причина отсутствия
- период начала и окончания отсутствия
- ссылка на карточку работника, за которым числится отсутствие

←

Absence

Редактирование элемента в Absence

Name

Ежегодный отпуск

Start Date

1 ноября 2024 г. ×

End Date

14 ноября 2024 г. ×

Pn Employee ID

NIKOLAEV NIKOLAY 1 января 1990 г. ✎ ×

Коллекция Anketa

Анкета содержит:

- ссылку на карточку физического лица
- фотографию кандидата
- ссылку на карточку справки
- вакансия, на которую претендует кандидат
- персональные данные и другая информация.

Anketa

← Редактирование элемента в Anketa

Pn Person ID

DMITRIEV DMITRIY 1 января 1990 г.

Anketa Photo

Pasted Image (2)



Pn Spravka ID

DMITRIEV DMITRIY DMIRIEVICH

Создать

Добавить существующий

Vacancy

ИТ-специалист

First Name

DMITRIY

Last Name

DMITRIEV

Birth

1990-01-01

Коллекция Spravka

Карточка справки по проверке кандидата содержит:

- ФИО кандидата
- ссылку на анкету
- персональные данные кандидата
- кем и когда осуществлялась проверка
- результат (статус) проверки и комментарий.

←

Sправка

Редактирование элемента в Sправка

Name

DMITRIEV DMITRIY DMIRIEVICH

Pn Anketa ID

DMITRIEV DMITRIY 1990-01-01

✎ ✕

Address

Россия, Санкт-Петербург

Phone

+7 911 00000

User Created

admin admin

When Created

14 декабря 2024 г. 16:07

Status

Согласовано

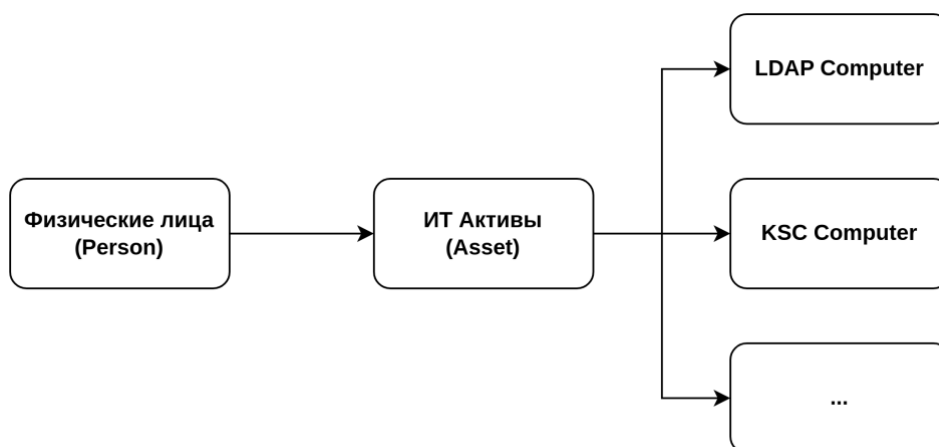
▼

Status Description

Негатива нет.

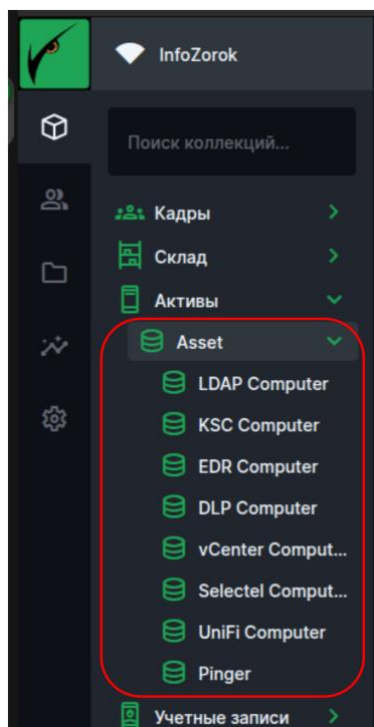
3.2.Модуль Активы

Модуль отвечает за консолидированные данные по всем ИТ-активам (компьютерам, серверам и др.), которые автоматизированно собираются в виде Объединяющей коллекции, нормализуются и связываются по ключевому полю serialnumber. Взаимосвязь коллекций:



В пункте меню модуля можно увидеть коллекции, входящие в его состав:

- Asset — Объединяющая коллекция
- LDAP Computer, KSC Computer и др. — коллекции-источники.



Коллекция Asset

Обобщающая коллекция Asset позволяет объединять данные по ИТ-активам из коллекций-источников и в едином интерфейсе предоставляет возможность оперативно переходить в источники для получения детальной информации. На рисунке ниже представлены возможности обобщающей коллекции.

	Name	Serialnumber	Person	Stock	LDAP	KSC	Infosystem
☐	DC01	sn21234567890	2 Элемента	1 Элемент	1 Элемент	1 Элемент	1 Элемент
☐	KSC01	sn01234567890	0 Элемент	1 Элемент	1 Элемент	1 Элемент	1 Элемент
☐	WS01	sn11234567890	1 Элемент	1 Элемент	1 Элемент	1 Элемент	Kaspersky Security Center
☐		sn31234567890	ROMANOV ROMAN	1 Элемент	0 Элемент	0 Элемент	0 Элемент

Каточка ИТ-актива содержит следующую информацию:

- серийный номер
- имя
- активный (не заблокирован), и существует в источниках

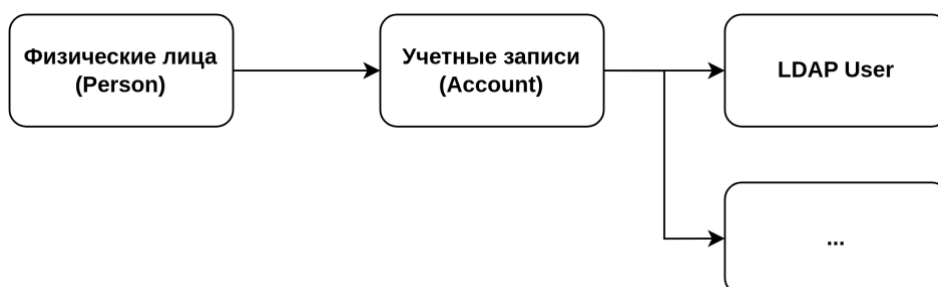
- поле для добавления комментариев
- ссылку на карточку информационной системы, к которой относится ИТ-актив
- ссылку на ответственного
- ссылки на карточки коллекций-источников, откуда информация была автоматизированно загружена.

Коллекции источники содержат ссылку на карточку ИТ-актива и все данные, которые были настроены при интеграции для экспорта. Например, для коллекции LDAP Computer, это CN, DistinguishedName, OperationSystem, ObjectSID и др.

3.3.Модуль Учетные записи

Модуль объединяет информацию из активных каталогов (LDAP) и кадровую информацию. Позволяет выполнять базовые функции IDM, такие как отслеживание приемов, увольнений и блокировки учетных записей, назначение ответственных за учетные записи.

Взаимосвязь коллекций:



В модуль входит обобщающая коллекция Учетные записи (Account) и коллекции-источники, в которые автоматизированно загружается информация из внешних систем.

Коллекция Account

Обобщающая коллекция Account позволяет автоматизированно объединять учетные записи по общему признаку (UserPrincipalName) из коллекций-источников и в едином интерфейсе предоставляет возможность оперативно переходить в источники для получения детальной информации. Возможности обобщающей коллекции:

	Userprincipalname	Displayname	Person	LDAP	Active	Exist
☐	☒ aalekseev@ab.loc	Alexey Alekseev	1 Элемент	1 Элемент	✓	✓
☐	☒ aalexandrov@ab.loc	Alexander Alexandrov	1 Элемент	1 Элемент	✗	✓
☐	☒ aanatolev@ab.loc	Anatoliy Anatolev	1 Элемент	aalexandrov@ab.loc ✗	✗	✓
☐	☒ aandreev@ab.loc	Andrey Andreev	1 Элемент	1 Элемент	✗	✓
☐	☒ Administrator@AB		ANDREEV ANDREY	1 Элемент	✗	✓
☐	☒ ddmित्रiev@ab.loc	Dmitriy Dmitriev	1 Элемент	1 Элемент	✓	✓
☐	☒ Guest@AB		0 Элементы	1 Элемент	✗	✓

Карточка учетной записи содержит:

- имя
- поле, по которому связываются учетные записи - UserPrincipalName
- признаки активна и удалена или учетная запись существует в источнике
- адрес электронной почты
- дата последней активности
- ссылки на карточки в коллекции-источнике
- ссылку на карточку ответственного за учетную запись.

Account
←
Редактирование элемента в Account

Displayname

Alexey Alekseev

Userprincipalname

aalekseev@ab.loc

Active

☒
Включено

Exist

☒
Включено

Mall

aalekseev@ab.com

Lastlogon

LDAP

aalekseev@ab.loc ✓

Person

ALEKSEEV ALEXY

Добавить существующий

Sys Group ID

Нет элементов

Создать

Добавить существующий

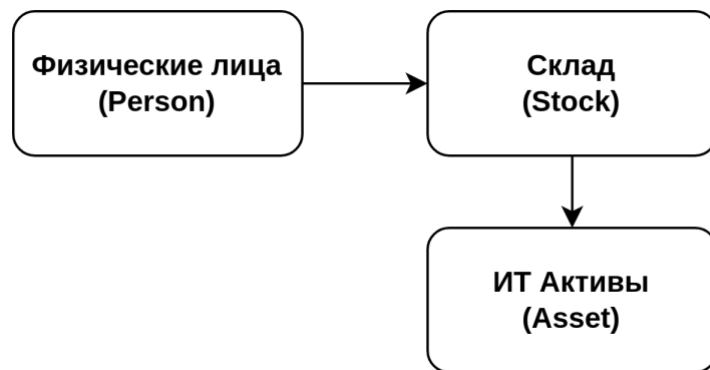
System Description

Коллекции источники содержат ссылку на карточку учетной записи (Account) и все данные, которые были настроены при интеграции для экспорта. Например, для коллекции LDAP User, это SamAccountName, DistinguishedName, LastLogonTimeStamp, ObjectSID и др.

3.4.Модуль Склад

Модуль позволяет вести учет материальных ценностей, с распределением по типам и назначением ответственных. Такие материальные ценности как, серверы и рабочие станции можно автоматизированно привязывать к Активам в соответствии с серийным номером.

Взаимосвязь коллекций показывает, как за материальные ценности назначаются ответственные, а материальные ценности, если они относятся к ИТ, привязываются к ИТ-Активам.



Коллекция Stock

Коллекция содержит данные:

- серийный номер
- тип
- имя, модель, конфигурацию и другие атрибуты
- ссылку на карточку ответственного физлица
- ссылку на карточку ИТ-актива

← Stock

Редактирование элемента в Stock

Serialnumber

sn11234567890

Sk Type ID

Notebook

✎ ✕

Name

📄

 Notebook Lenovo ThinkPad E14

Model

ThinkPad E14

Configuration

I7/16GB RAM /512 SSD

When Created

7 апреля 2024 г. ✕

Status ^{*}

granted ▾

When Granted

📅

Inventorynumber

Location

Organization

ABSERVICE ▾

Responsible person

NIKOLAEV NIKOLAY ✕

At Asset ID

📄

 WS01

✎ ✕

Добавить существующий

Description

3.3.Модуль Документы

Позволяет регистрировать нормативные документы компании и контролировать ознакомление с ними работников.

Коллекция Документы

В списке коллекции можно учитывать все документы для ознакомления и сколько работников с ними ознакомились:

Контент

Document

	Name	Number	Date Created	Version	Pn Employee ID
☐	☐ Политика информационной безопасности	N2-2024-03-31	около 1 года наз...	1	1 Элемент
☐	☐ Соглашение о неразглашении	N1-2024-03-31	около 1 года наз...	1	2 Элемента

NIKOLAEV NIKOLAY ABSERVICE

DMITRIEV DMITRIY ABSERVICE

Карточка документа содержит:

- название и реквизиты документа
- кем и когда создан
- ссылка на загруженный в систему документ
- ссылки на карточки работников, которые ознакомлены с документом

Document

← Редактирование элемента в Document

Number *

N2-2024-03-31

Version *

1

Date Created

31 марта 2024 г. 09:32

User Created

admin admin

Name *

Политика информационной безопасности

Directus Files ID

Файл не выбран

Pn Employee ID

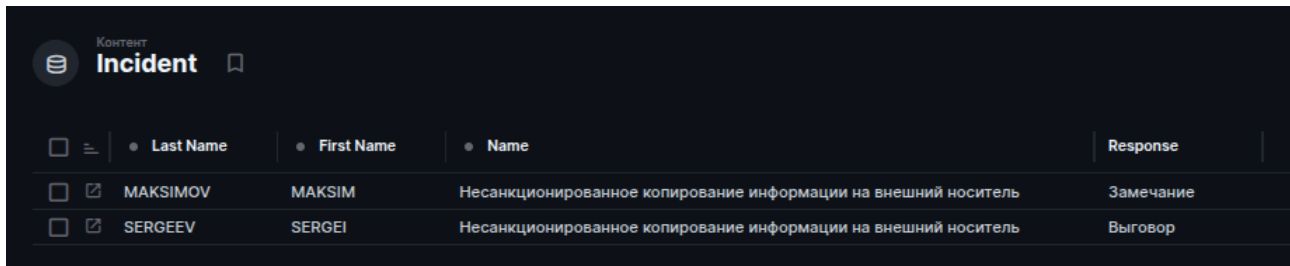
NIKOLAEV NIKOLAY ABSERVICE

Добавить существующий

3.4.Модуль Инциденты

Модуль позволяет регистрировать, разделять по категориям, привязывать нарушителей и их руководителей к выявленным инцидентам.

Коллекция Инциденты



The screenshot shows a web interface for the 'Incident' module. At the top, there is a header with a menu icon, the word 'Контент' (Content), and the title 'Incident' with a bookmark icon. Below the header is a table with columns for selection, last name, first name, name, and response. Two incidents are listed: one for MAKSIMOV with a 'Замечание' (Remark) response, and one for SERGEEV with a 'Выговор' (Reprimand) response. Both incidents are categorized as 'Несанкционированное копирование информации на внешний носитель' (Unauthorized copying of information to an external carrier).

☐	☐	• Last Name	• First Name	• Name	Response
☐	☒	MAKSIMOV	MAKSIM	Несанкционированное копирование информации на внешний носитель	Замечание
☐	☒	SERGEEV	SERGEI	Несанкционированное копирование информации на внешний носитель	Выговор

Карточка инцидента содержит:

- ссылки на карточки работников, нарушителя и его руководителя
- даты совершения и выявления инцидента
- тип
- описание и решение по результату обработки
- кем был зарегистрирован инцидент

← It Incident

Редактирование элемента в It Incident

Pn Person ID Intruder

MAKSIMOV MAKSIM 1 января 1990 г.  

Добавить существующий

Pn Person ID Head

DMITRIEV DMITRIY 1 января 1990 г.  

Добавить существующий

When Occured

13 марта 2024 г. 12:00 

When Detected

13 марта 2024 г. 12:00 

It Type ID *

Несанкционированное копирование информации на внешний носитель  

Summary

Работник скопировал рабочие файлы на флэшку.

Response

Замечание 

User Created

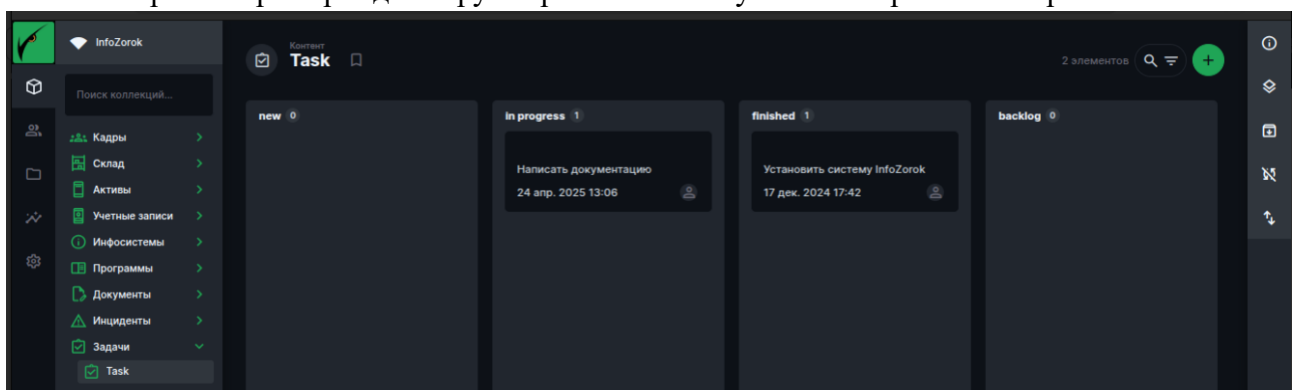
admin admin

3.5.Модуль Задачи

Модуль позволяет регистрировать задачи, назначать их на ответственных, отслеживать сроки исполнения.

Коллекция Задачи

Ниже изображен пример задач с группировкой по статусам и отображением краткого описания.



- название
- ответственный за выполнение
- статус
- даты начала и завершения
- детальное описание.

Система позволяет добавить ссылки на карточки объектов системы. Таким образом можно связывать с задачей активы, учетные записи по которым проводятся работы и т. д.

При возникновении вопросов по работе системы вы можете обратиться к администратору системы в вашей организации, или в техническую поддержку вендора по адресу электронной почты support@ib-nova.ru .